UNIVERSITY OF BIRMINGHAM
University of Birmingham Research at Birmingham

# First fall degree and Weil descent

Hodges, Timothy J.; Petit, Christophe; Schlather, Jacob

*DOI:*
10.1016/j.ffa.2014.07.001

*License:*
Other (please provide link to licence statement

*Document Version*
Publisher's PDF, also known as Version of record

*Citation for published version (Harvard):*
Hodges, TJ, Petit, C & Schlather, J 2014, 'First fall degree and Weil descent', *Finite Fields and Their Applications*, vol. 30, pp. 155-177. https://doi.org/10.1016/j.ffa.2014.07.001

Link to publication on Research at Birmingham portal

**General rights**
Unless a licence is specified above, all rights (including copyright and moral rights) in this document are retained by the authors and/or the copyright holders. The express permission of the copyright holder must be obtained for any use of this material other than for purposes permitted by law.

•Users may freely distribute the URL that is used to identify this publication.
•Users may download and/or print one copy of the publication from the University of Birmingham research portal for the purpose of private study or non-commercial research.
•User may use extracts from the document in line with the concept of 'fair dealing' under the Copyright, Designs and Patents Act 1988 (?)
•Users may not further distribute the material nor use it for the purposes of commercial gain.

Where a licence is displayed above, please note the terms and conditions of the licence govern your use of this document.

When citing, please reference the published version.

**Take down policy**
While the University of Birmingham exercises care and attention in making items available there are rare occasions when an item has been uploaded in error or has been deemed to be commercially or otherwise sensitive.

If you believe that this is the case for this document, please contact UBIRA@lists.bham.ac.uk providing details and we will remove access to the work immediately and investigate.

Download date: 05. May. 2023

Finite Fields and Their Applications 30 (2014) 155–177

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# First fall degree and Weil descent

Timothy J. Hodges [a,*,1], Christophe Petit [b,2], Jacob Schlather [a]

[a] *University of Cincinnati, Cincinnati, OH 45221-0025, USA*
[b] *Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium*

ARTICLE INFO

*Article history:*
Received 18 January 2013
Received in revised form 8 July 2014
Accepted 9 July 2014
Available online 26 July 2014
Communicated by Igor Shparlinski

*MSC:*
primary 11T55
secondary 11T71, 11Y16, 12Y05, 13D02, 94A60

*Keywords:*
First fall degree
Weil descent
Finite field
Degree of regularity

ABSTRACT

Polynomial systems arising from a Weil descent have many applications in cryptography, including the HFE cryptosystem and the elliptic curve discrete logarithm problem over small characteristic fields. Understanding the exact complexity of solving these systems is essential for the applications. A first step in that direction is to study the *first fall degree* of the systems. In this paper, we establish a rigorous general bound on the first fall degree of polynomial systems arising from a Weil descent. We also provide experimental data to study the tightness of our bound in general and its plausible consequences on the complexity of polynomial systems arising from a Weil descent.

© 2014 Elsevier Inc. All rights reserved.

## 1. Introduction

The problem of finding solutions to systems of polynomial equations over a finite field arises in many aspects of mathematics and in particular in cryptography. In this paper,

* Corresponding author at: Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221-0025, USA.
*E-mail addresses:* timothy.hodges@uc.edu (T.J. Hodges), christophe.petit@uclouvain.be (C. Petit), jacob.schlather@gmail.com (J. Schlather).

[1] The first author was supported by a grant from the Charles P. Taft Research Center.
[2] The second author was supported by an F.R.S. - FNRS postdoctoral research grant.

http://dx.doi.org/10.1016/j.ffa.2014.07.001
1071-5797/© 2014 Elsevier Inc. All rights reserved.

we consider the situation where the system arises from a Weil descent on a polynomial operator of given degree on an extension field.

More precisely, let $\mathbb{F}$ be a finite field of order $q$ and let $\mathbb{K}$ be an extension of $\mathbb{F}$ of degree $n$. Let $P\colon \mathbb{K}^m \to \mathbb{K}$ be a polynomial function. Through the identification $\mathbb{K} \cong \mathbb{F}^n$, an equation of the form $P(X) = Y$ becomes a system of equations $p_1(x_{11}, \ldots, x_{mn}) = y_1$, $\ldots, p_n(x_{11}, \ldots, x_{mn}) = y_n$ over the base field $\mathbb{F}$. The polynomial $P$ has two degrees, one over $\mathbb{K}$ which is the degree of $P$ as a polynomial over $\mathbb{K}$ and one as a polynomial operator on the $\mathbb{F}$-vector space $\mathbb{K}$. We set $D = \deg_{\mathbb{K}} P$ and $d = \deg_{\mathbb{F}} P$. For instance, if $q = 2$ and $P(X) = X^7 + X^5 + 1$ then $D = 7$ and $d = 3$ since the functions $X^{2^i}$ are all linear over $\mathbb{F}$.

When $P$ is quadratic over the base field, the polynomial $P$ and the corresponding system form the basic structure behind Patarin's HFE cryptosystem [19]. This particular case is now reasonably well understood [2,7,6,9,16]. Various generalizations of the HFE cryptosystem have been proposed involving operators $P$ with higher degree over the base field [20,21,25]. Higher degree operators also arise in Diem's algorithm for the discrete logarithm problem on binary elliptic curves and in the factorization problem for $SL(2, \mathbb{F}_{2^n})$ [14,15,22].

One particularly effective approach to solving a polynomial system of equations is to apply a Gröbner basis algorithm such as Faugère's $F_4$ or $F_5$ [11,12]. In order to understand the complexity of this approach, we need to know the *degree of regularity* of the system, which is the highest degree polynomial that occurs in the algorithm before it successfully terminates. Since this degree is hard to determine precisely we use a proxy, the *first fall degree*. The first fall degree is defined to be the first degree at which non-trivial relations between the $p_i$ occur; the trivial relations being relations such as $p_i p_j - p_j p_i = 0$ and $(p_i^{q-1} - 1)p_i = 0$.

*Contributions of this paper.* We find a bound on the first fall degree of systems of equations arising from a multivariate polynomial operator. In particular if the operator is univariate of degrees $D$ and $d$ over the fields $\mathbb{K}$ and $\mathbb{F}$ respectively, then our bound is

$$D_{\text{ff}} \leq \frac{(q-1)\log_q(D-d+1) + q + d + 1}{2}$$

This generalizes the result in [6] where the bound when $d = 2$ was given as

$$D_{\text{ff}} \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2 = \frac{(q-1)\lfloor \log_q(D-1) \rfloor + q + 3}{2}$$

Our bound also generalizes the bound in [22] for multivariate polynomials over $\mathbb{F}_2$. In that paper it was shown that if the operator has degree at most $2^t - 1$ over $\mathbb{K}$ in any of the $m$ variables, then the first fall degree is bounded by $mt + 1$. Our bound easily implies this bound as well as its generalization to an arbitrary base field of order $q$: if the operator has degree at most $q^t - 1$ in any of the $m$ variables, then the first fall degree is bounded by $(q-1)mt + 1$. Moreover, our result gives a much sharper bound than

that given in [22] when the degree $d$ over $\mathbb{F}$ is smaller than for random polynomials with degree $D$ over $\mathbb{K}$.

We then experimentally study these systems using the Gröbner basis routine of the Magma computer algebra system. Our experimental results suggest that our bound can probably be slightly improved in general. Further results also suggest that the first fall degree of these systems might be a good approximation of their degree of regularity in general, an assumption taken in several previous works on similar systems. We note that under this heuristic assumption, Gröbner basis attacks on generalizations of HFE systems to operators of higher degree would have quasi-polynomial time complexity. This generalizes the result of Ding and Hodges [6] in the case when $d = 2$. Under the assumption of a variant of Fröberg's conjecture, subexponential complexity was also established for the Kipnis–Shamir MinRank attack on HFE systems over an arbitrary base field by Bettale, Faugère and Perret in [2,3]. For the case of HFE with $d = 2$, the bound on the degree of regularity for this approach is substantially better ($\approx \log_q(D)$) than the bound provided here ($\approx q \log_q(D)$) for the first fall degree.

## 2. First fall degree

We first introduce the notion of first fall degree in a fairly abstract setting. Let $\mathbb{F}$ be a finite field of characteristic $p$. Let $A$ be a finite dimensional filtered algebra over $\mathbb{F}$; that is there exist a positive integer $N$ and subspaces $A_0 \subset A_1 \subset \cdots \subset A_N = A$ such that $A_i A_j \subset A_{i+j}$. The degree of an element $a \in A$ is defined to be the smallest $d$ such that $a \in A_d$. Suppose also that there exists a power of $p$, $q = p^m$ such that for all elements $a$ of degree $d \geq 1$, $\deg a^q < dq$. The canonical example of such an object is the ring of functions from $\mathbb{F}^n$ to $\mathbb{F}$; here $A \cong \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$ where $q = |\mathbb{F}|$.

A degree fall for a subspace $V$ of $A$ is a combination of multiples of elements of $V$ whose degree is less than the expected bound. That is, it is a combination $\sum a_i v_i$ whose degree is less than $\max\{\deg a_i + \deg v_i\}$. Such combinations can be thought of as formal combinations $\sum a_i \otimes v_i$ in the tensor product $A \otimes V$ with evaluation of the combination in $A$ given by the linear map $\psi\colon A \otimes V \to V$ such that $\psi(\sum a_i \otimes v_i) = \sum a_i v_i$. There are a number of degree falls that we want to ignore because they occur for trivial reasons. If $\deg v = \deg w = d$ and $v - v' \in A_{d-1}$ and $w - w' \in A_{d-1}$ (so $v$ and $v'$ have the same highest degree term in some sense) then $w' \otimes v - v' \otimes w$ is a degree fall. Also for any $v \in A$, $v^{q-1} \otimes v$ is a degree fall. We are interested in degree falls that are not combinations of such trivial degree falls and particularly in the first degree at which a non-trivial degree fall exists.

More formerly, degree falls of degree $k$ will be elements of the kernel of the composed map

$$A_{k-d} \otimes V \to \frac{A_{k-d}V}{(A_{k-d}V) \cap A_{k-d-1}} \cong \frac{A_{k-d}V + A_{k-d-1}V}{A_{k-d-1}}$$

This kernel obviously also contains $A_{k-d-1} \otimes V$ and we want to ignore this part of it; so we should consider the domain of the map as

$$\frac{A_{k-d} \otimes V}{A_{k-d-1} \otimes V} \cong \frac{A_{k-d}}{A_{k-d-1}} \otimes V$$

Thus the degree falls are the kernel of the map

$$\psi\colon \frac{A_{k-d}}{A_{k-d-1}} \otimes V \to \frac{A_{k-d}V + A_{k-d-1}V}{A_{k-d-1}}$$

The trivial degree falls are a subspace of the kernel and the non-trivial degree falls can be considered as the quotient of the kernel by the space of trivial degree falls. At this point it becomes apparent that the degree falls are best approached through the associated graded ring. This is the algebra $\operatorname{Gr} A$ defined to be the vector space $\bigoplus_j A_j/A_{j-1}$ equipped with multiplication defined in the following way. If $\deg(a) = d$, and $\deg(a') = d'$, then $(a + A_{d-1}).(a' + A_{d'-1}) = aa' + A_{d+d'-1}$.

Thus rather than giving a formal definition of first fall degree in a filtered algebra, we shall define it in a graded algebra and then pull back this information to the original ring from the associated graded ring.

Denote by $B = \bigoplus_{k=0}^{N} B_k$ a graded finite dimensional algebra over $\mathbb{F}$. That is, $B$ is the direct sum of the subspaces $B_k$ and $B_j B_k \subset B_{j+k}$. Suppose further that there exists a $q = p^m$ such that $b^q = 0$ for all $b \in \bigoplus_{k=1}^{N} B_k$. A homogeneous subspace of $B$ is a subspace $V \subset B_d$ for some $d$. If $V$ and $W$ are $\mathbb{F}$-vector spaces, we denote by $V \otimes W$ the tensor product of $V$ and $W$. If $V$ is a homogeneous subspace of degree $d$, we have linear maps $\phi_j\colon B_j \otimes V \to B_j V$ for all $j = 0, \ldots, N$ given by $\phi_j(\sum_i b_i \otimes v_i) = \sum_i b_i v_i$. Let $R_j(V) = \ker \phi_j$. This yields an exact sequence

$$0 \longrightarrow R_j(V) \longrightarrow B_j \otimes V \longrightarrow B_j V \longrightarrow 0$$

Inside $R_j(V)$ there is a subspace of "trivial relations" $T_j(V)$ spanned by the elements

(1) $b(v \otimes w - w \otimes v)$ where $v, w \in V$ and $b \in B_{j-d}$;
(2) $b(v^{q-1} \otimes v)$ where $v \in V$ and $b \in B_{j-(q-1)d}$.

**Definition 2.1.** For a homogeneous subspace $V \subset B_d$, we define the *first fall degree* of $V$ to be the first degree at which non-trivial relations occur

$$D_{\mathrm{ff}}(V) = \min\{j \mid T_{j-d}(V) \subsetneq R_{j-d}(V)\}$$

We now return to the case of a filtered algebra $A$ as defined above. For any subspace $V$ of $A_d$ we define $\bar{V} = (V + A_{d-1})/A_{d-1} \subset A_d/A_{d-1}$. If $V \cap A_{d-1} \neq 0$, then there are $\mathbb{F}$-linear combinations of elements of $V$ that have degree less than $d$, so the first fall

degree is $d$. Since this information is lost in the passage from $V$ to $\bar{V}$, we define the first fall degree to be $d$ in this case and otherwise to be the first fall degree of $\bar{V}$.

**Definition 2.2.** For a subspace $V \subset A_d$, we define the *first fall degree* of $V$ by

$$D_{\text{ff}}(V) = \begin{cases} d & \text{if } \dim \bar{V} < \dim V \\ D_{\text{ff}}(\bar{V}) & \text{otherwise} \end{cases}$$

We will also use the notation $D_{\text{ff}}(p_1, \ldots, p_n)$ to mean $D_{\text{ff}}(V)$ where $V$ is the vector space spanned by the $p_i$.

Let us note a couple of important general properties of the first fall degree of graded algebras. Both of these results are proved in [7] in the specific case they were considering. These proofs extend easily to the more general framework we are considering. For the sake of completeness we provide full details. We first note that extension of the base field does not affect the first fall degree.

**Lemma 2.3.** *Let $B$ be a graded algebra over $\mathbb{F}$, let $\mathbb{K}$ be an extension field of $\mathbb{F}$ and let $\tilde{B} = \mathbb{K} \otimes_{\mathbb{F}} B$. Let $\tilde{V} = \mathbb{K} \otimes_{\mathbb{F}} V \subset \tilde{B}$. Then $D_{\text{ff}}(V) = D_{\text{ff}}(\tilde{V})$.*

**Proof.** Notice that the $D_{\text{ff}}(V)$ is the smallest $j$ such that the sequence

$$0 \longrightarrow T_{j-d}(V) \longrightarrow B_{j-d} \otimes_{\mathbb{F}} V \longrightarrow B_{j-d}V \longrightarrow 0$$

is not exact, while $D_{\text{ff}}(\tilde{V})$ is the smallest $j$ such that the sequence

$$0 \longrightarrow T_{j-d}(\tilde{V}) \longrightarrow \tilde{B}_{j-d} \otimes_{\mathbb{K}} \tilde{V} \longrightarrow \tilde{B}_{j-d}\tilde{V} \longrightarrow 0$$

is not exact. Observe that $\tilde{B}_{j-d} \otimes_{\mathbb{K}} \tilde{V} = \mathbb{K} \otimes_{\mathbb{F}} B_{j-d} \otimes_{\mathbb{F}} V$ and $\tilde{B}_{j-d}\tilde{V} = \mathbb{K} \otimes_{\mathbb{F}} B_{j-d}V$. Moreover $T_{j-d}(\tilde{V}) = \mathbb{K} \otimes_{\mathbb{F}} T_{j-d}(V)$. Thus the second sequence identifies with the sequence

$$0 \longrightarrow \mathbb{K} \otimes_{\mathbb{F}} T_{j-d}(V) \longrightarrow \mathbb{K} \otimes_{\mathbb{F}} B_{j-d} \otimes_{\mathbb{F}} V \longrightarrow \mathbb{K} \otimes_{\mathbb{F}} B_{j-d}V \longrightarrow 0$$

By the exactness of the tensor product, this sequence is exact if and only if the first sequence is. □

Since extension of the base field commutes with passage to the associated graded algebra, we have an analogous result for filtered algebras.

**Corollary 2.4.** *Let $A$ be a filtered algebra over $\mathbb{F}$, let $\mathbb{K}$ be an extension field of $\mathbb{F}$ and let $\tilde{A} = \mathbb{K} \otimes_{\mathbb{F}} A$. Let $V \subset A_d$ and let $\tilde{V} = \mathbb{K} \otimes_{\mathbb{F}} V \subset \tilde{A}$. Then $D_{\text{ff}}(V) = D_{\text{ff}}(\tilde{V})$.*

Secondly, the first fall degree of a subspace is at least that of the original space.

**Definition 2.5.** Let $V \subset B_d$ be a subspace of dimension $m$; let $V'$ be a subspace of $V$ of dimension $m-1$ and let $v_m \in V \backslash V'$. Define

$$T_k^s(V) = \left\{ \xi \in B_k \otimes V' \;\middle|\; \exists c \in B_{k-d(q-s)} \text{ such that } \xi + c v_m^{q-s} \otimes v_m \in T_k(V) \right\}$$

Note that $T_k^1(V) = B_k \otimes V' \cap T_k(V)$. Our aim is to show that $T_k^1(V) \subset T_k(V')$.

**Lemma 2.6.** *If $k < D_{\mathrm{ff}}(V)$, then for $s \geq 1$,*

$$T_k^s(V) \subset T_k\big(V'\big) + v_m T_{k-d}^{s+1}(V)$$

**Proof.** Let $\{v_1, \ldots, v_{m-1}\}$ be a basis for $V'$. Let $\xi \in T_k^s(V)$ so that $\xi + c v_m^{q-s} \otimes v_m \in T_k(V)$ for some $c$. Then,

$$\xi + c v_m^{q-s} \otimes v_m = \sum_{i<j} b_{ij}(v_i \otimes v_j - v_j \otimes v_i) + \sum_i c_i v_i^{q-1} \otimes v_i$$

Set

$$L = \sum_{1 \leq i < j \leq m-1} b_{ij}(v_i \otimes v_j - v_j \otimes v_i) + \sum_{i=1}^{m-1} c_i v_i^{q-1} \otimes v_i \in T_k\big(V'\big)$$

Then

$$\begin{aligned} \xi - L + \sum_{i<m} b_{im} v_m \otimes v_i &= \sum_{i<m} b_{im} v_i \otimes v_m + c_m v_m^{q-1} \otimes v_m - c v_m^{q-s} \otimes v_m \\ &\in B_k \otimes V' \cap B_k \otimes v_m = 0 \end{aligned}$$

So

$$\xi = L - \sum_{i<m} b_{im} v_m \otimes v_i = L - v_m \sum_{i<m} b_{im} \otimes v_i$$

and

$$\sum_{i<m} b_{im} v_i \otimes v_m + c_m v_m^{q-1} \otimes v_m - c v_m^{q-s} \otimes v_m = 0$$

The latter equation implies that

$$\sum_{i<m} b_{im} v_i + c_m v_m^{q-1} - c v_m^{q-s} = 0$$

and hence that

$$\sum_{i<m} b_{im} \otimes v_i + c_m v_m^{q-2} \otimes v_m - c v_m^{q-s-1} \otimes v_m \in R_{k-d}(V) = T_{k-d}(V)$$

since $k < D_{\mathrm{ff}}(V)$. Thus

$$\sum_{i<m} b_{im} \otimes v_i + \big(c_m v_m^{s-1} - c\big) v_m^{q-s-1} \otimes v_m \in T_{k-d}(V)$$

so $\sum_{i<m} b_{im} \otimes v_i \in T_{k-d}^{s+1}$. Thus $\xi \in T_k(V') + v_m T_{k-d}^{s+1}(V)$ as claimed. □

**Theorem 2.7.** *For any subset $V' \subset V$, $B_k \otimes V' \cap T_k(V) = T_k(V')$ for $k < D_{\mathrm{ff}}(V)$.*

**Proof.** It suffices to prove the result in the case where $\dim V/V' = 1$. Iterating the lemma yields that

$$B_k \otimes V' \cap T_k(V) = T_k^1(V) \subset T_k\big(V'\big) + v_m^s T_{k-sd}^{s+1}(V)$$

Eventually the term $v_m^s T_{k-sd}^{s+1}(V)$ will be zero because either $v_m^s = 0$, or $T_{k-sd} = 0$. Thus $B_k \otimes V' \cap T_k(V) \subset T_k(V')$. The opposite inclusion is trivial. □

**Theorem 2.8.** *Let $B$ be a graded algebra. Let $V$ be a homogeneous subspace and let $V'$ be a subspace of $V$. Then $D_{\mathrm{ff}}(V) \leq D_{\mathrm{ff}}(V')$.*

**Proof.** If $k \leq D_{\mathrm{ff}}(V)$, then $R_{k-d}(V') \subset B_{k-d} \otimes V' \cap T_{k-d}(V) = T_{k-d}(V')$ by Theorem 2.7. Hence $D_{\mathrm{ff}}(V') \geq D_{\mathrm{ff}}(V)$. □

## 3. Multivariate operators

Suppose that $\mathbb{F}$ is a field with $q$ elements and $\mathbb{K}$ is an extension of $\mathbb{F}$ of degree $n$ so that $|\mathbb{K}| = q^n$. Set $A = \mathrm{Fun}(\mathbb{K}^m, \mathbb{K}) = \mathbb{K}[X_1, \ldots, X_m]$ where $X_j^{q^n} = X_j$. Consider a multivariate polynomial function $P(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$. Fix a dual basis for $\mathbb{K}$ over $\mathbb{F}$:

$$\big\{(e_i, x_i), i = 1, \ldots, n \;\big|\; e_i \in \mathbb{K},\ x_i \in \mathbb{K}^* = \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{F})\big\}$$

where $\sum_i x_i(z) e_i = z$ for all $z \in \mathbb{K}$. Identify $\mathbb{K}$ with $\mathbb{F}^n$ via the linear isomorphism $z \mapsto (x_1(z), \ldots, x_n(z))$ and set

$$p_i = x_i \circ P : \mathbb{K}^m \to \mathbb{F}$$

Then $P$ identifies with the system of multivariate functions $(p_1, \ldots, p_n) : \mathbb{K}^m \to \mathbb{F}^n$.

Let $\pi_j : \mathbb{K}^m \to \mathbb{K}$ be the $j$-th projection. Define $x_{ji} : \mathbb{K}^m \to \mathbb{F}$ by $x_{ji} = x_i \circ \pi_j$ and let

$$A_{\mathbb{F}} = \mathrm{Fun}\big(\mathbb{K}^m, \mathbb{F}\big) = \mathbb{F}[x_{11}, \ldots, x_{1n}, \ldots, x_{m1}, \ldots, x_{mn}]$$

Note that $x_{ji}^q = x_{ji}$.

We are interested in understanding the first fall degree of the system $\{p_1, \ldots, p_n\}$ in terms of properties of the operator $P$. The connection lies in the fact that

$$A = \mathrm{Fun}\big(\mathbb{K}^m, \mathbb{K}\big) = \mathbb{K} \otimes_{\mathbb{F}} \mathrm{Fun}\big(\mathbb{K}^m, \mathbb{F}\big) = \mathbb{K} \otimes_{\mathbb{F}} A_{\mathbb{F}}$$

Let $V = \sum_i \mathbb{F}p_i \subset A_{\mathbb{F}}$. As observed in Corollary 2.4, the first fall degree of $V$ is the same as the first fall degree of $\mathbb{K} \otimes_{\mathbb{F}} V = \sum_i \mathbb{K}p_i$ calculated in $\mathbb{K} \otimes_{\mathbb{F}} A_{\mathbb{F}} = A$. The following result is well-known and has been observed in varying forms by many authors. It is an easy consequence of Artin's Lemma on independence of characters [18, Lemma 2.33].

**Lemma 3.1.** $\sum_i \mathbb{K}p_i = \sum_i \mathbb{K}P^{q^i}$.

**Proof.** First note that when $m = 1$ we have

$$\mathbb{K}[X] = \mathrm{Fun}(\mathbb{K}, \mathbb{K}) = \mathbb{K} \otimes_{\mathbb{F}} \mathrm{Fun}(\mathbb{K}, \mathbb{F}) = \mathbb{K}[x_1, \ldots, x_n]$$

and that the space of $\mathbb{F}$-linear maps is $\sum_i \mathbb{K}X^{q^i} = \sum_i \mathbb{K}x_i$. Since $x_i \circ P = p_i$ and $X^{q^i} \circ P = P^{q^i}$, it follows that

$$\begin{aligned}
\sum_i \mathbb{K}p_i &= \left\{ L \circ P \;\middle|\; L \in \sum_i \mathbb{K}x_i \right\} \\
&= \left\{ L \circ P \;\middle|\; L \in \sum_i \mathbb{K}X^{q^i} \right\} \\
&= \sum_i \mathbb{K}P^{q^i} \qquad \square
\end{aligned}$$

Thus the first fall degree of the subspace $V = \sum_i \mathbb{F}p_i$ of $A_{\mathbb{F}}$ is equal to the first fall degree of the subspace $V_{\mathbb{K}} = \sum \mathbb{K}P^{q^i}$ of $A$ equipped with the filtration by degree over $\mathbb{F}$. That is,

$$A_0 = \mathbb{K}, \qquad A_1 = \sum_{i,j} \mathbb{K}X_j^{q^i} + \mathbb{K}, \qquad A_{i+1} = A_1 A_i$$

Denote the associated graded ring of $A$ with respect to this filtration by $B = \bigoplus A_i/A_{i-1}$. Define $X_{ij} = X_j^{q^i} + A_0 \in B_1 = A_1/A_0$ for $i = 0, \ldots, n-1$ and $j = 1, \ldots, m$. Then

$$B = \mathbb{K}[X_{01}, \ldots, X_{n-1,m}]$$

where $X_{jk}^q = 0$ for all $j$ and $k$.

**Definition 3.2.** Suppose that $P(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$ has degree $d$ over $\mathbb{F}$. The $P^{q^i}$ also has degree $d$ over $\mathbb{F}$ so $P^{q^i} \in A_d$. We define $P_i = P^{q^i} + A_{d-1} \in B_d = A_d/A_{d-1}$. In particular, $P_0 = P + A_{d-1} \in B_d$.

For example if $P$ is the quadratic operator $P(X_1,\dots,X_m) = X_1X_1^{q^{\theta_1}} + \cdots + X_mX_m^{q^{\theta_m}}$ then $P_0 = X_{01}X_{\theta_1,1} + \cdots + X_{0m}X_{\theta_m,m}$.

**Theorem 3.3.** *Let $P(X_1,\dots,X_m) \in \mathbb{K}[X_1,\dots,X_m] = \mathrm{Fun}(\mathbb{K}^m,\mathbb{K})$. Let $\{x_1,\dots,x_n\}$ be a basis for $\mathrm{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{F})$ and let $p_i = x_i \circ P$. Let $P_0$ be as defined above. Then*

$$D_{\mathrm{ff}}\big(\{p_1,\dots,p_n\}\big) \le D_{\mathrm{ff}}(P_0)$$

**Proof.** Using Corollary 2.4, Theorem 2.8 and Lemma 3.1, we have

$$\begin{aligned} D_{\mathrm{ff}}\big(\{p_1,\dots,p_n\}\big) &= D_{\mathrm{ff}}\left(\sum_i \mathbb{F}p_i\right) = D_{\mathrm{ff}}\left(\sum_i \mathbb{K}p_i\right) = D_{\mathrm{ff}}\left(\sum_i \mathbb{K}P^{q^i}\right) \\ &= D_{\mathrm{ff}}\left(\sum_i \mathbb{K}P_i\right) \le D_{\mathrm{ff}}(P_0) \qquad \square \end{aligned}$$

## 4. First fall degree of a single polynomial

Let $q$ be a power of a prime, let $\mathbb{K}$ be a finite field whose order is divisible by $q$ and let $B = \mathbb{K}[X_1,\dots,X_n]/\langle X_1^q,\dots,X_n^q\rangle$. Let $N = n(q-1)$, the largest possible degree of an element of $B$. Let $\lambda$ be a homogeneous element of degree $d$. Since $\lambda^{q-r}\lambda^r = \lambda^q = 0$, for any positive integer $m$ we have a complex of the form

$$\cdots \xrightarrow{\lambda^{q-r}} B_{m-dq} \xrightarrow{\lambda^r} B_{m-d(q-r)} \xrightarrow{\lambda^{q-r}} B_m \xrightarrow{\lambda^r} B_m\lambda^r \qquad (*)$$

(Recall that in a complex the image of one map is contained, but not necessarily equal to, the kernel of the next map.) The homology spaces of a complex are defined to be the kernel of one map factored out by the image of the previous one. We denote the homology spaces for this complex by

$$H\big(\lambda^r, B_k\big) = \frac{\mathrm{Ann}(\lambda^{q-r}) \cap B_k}{\lambda^r B_{k-rd}}$$

Note that $\mathrm{Ann}(\lambda^{q-r}) \cap B_k$ is the set of all annihilators of $\lambda^{q-r}$ of degree $k$ and $\lambda^r B_{k-rd}$ is the space of trivial annihilators of $\lambda^{q-r}$ of degree $k$. Thus the homology $H(\lambda^{q-1}, B_k)$ can be thought of as the vector space of non-trivial relations on $\lambda$ and is non-zero if and only if there is a non-trivial degree fall at degree $k+d$. Moreover

$$D_{\mathrm{ff}}(\lambda) = \min\big\{k \;\big|\; H\big(\lambda^{q-1}, B_k\big) \neq 0\big\} + d$$

If all the homology spaces are zero (that is, the complex is exact), the dimension of $B_m\lambda^r$ can be calculated as the alternating sum

$$\dim B_m\lambda^r = \dim B_m - \dim B_{m-d(q-r)} + \dim B_{m-dq} - \dim B_{m-dq-d(q-r)} + \cdots$$

Recall that $\dim B_k$, being the number of ways of arranging $k$ objects into $n$ cells with at most $q-1$ objects in each cell, is the generalized binomial coefficient $C_q(n,k)$ – the coefficient of $z^k$ in the expansion of $(1+z+\cdots+z^{q-1})^n$ [23, p. 104]. If the complex is exact, the dimension of $B_k\lambda^r$ is given by

$$\begin{aligned}\dim B_k\lambda^r &= C_q(n,k) - C_q\big(n,k-d(q-r)\big) + C_q(n,k-dq) - \cdots \\ &= \sum_{j=0}^{\lfloor k/dq\rfloor} C_q(n,k-jdq) - C_q\big(n,k-d(q-r)-jdq\big)\end{aligned}$$

Define

$$\gamma_q(n,d,r,k) = \sum_{j=0}^{\lfloor k/dq\rfloor} C_q(n,k-jdq) - C_q(n,k-rd-jdq)$$

(If we make the convention that $C_q(n,k)=0$ for $k<0$, we can equally well write the summation as $\sum_{j=0}^{\infty}$ since the terms for $j>\lfloor k/dq\rfloor$ are all zero.) In this notation, if our complex is exact,

$$\dim B_k\lambda^r = \gamma_q(n,d,q-r,k)$$

We also want to consider the same summation extending in both directions, so we define

$$\Gamma_q(n,d,r,k) = \sum_{j=-\infty}^{\infty} C_q(n,k-jdq) - C_q(n,k-rd-jdq)$$

For fixed $q,n,d$ and $r$, $\Gamma_q(n,d,r,k)$ is a $qd$-periodic function of $k$. We begin by collecting together some elementary properties of these functions.

**Lemma 4.1.**

(1) $\gamma_q(n,d,r,k) = C_q(n,k) - \gamma_q(n,d,q-r,k-dr)$.
(2) $\Gamma_q(n,d,r,k) = \gamma_q(n,d,r,k) - \gamma_q(n,d,r,N-d(q-r)-k)$.

**Proof.** Part (1) follows immediately from the definition. For part (2) observe that $C_q(n,k) = C_q(n,N-k)$ so that

$$\begin{aligned}&\gamma_q\big(n,d,r,N-d(q-r)-k\big) \\ &\quad= \sum_{j=0}^{\infty}\big[C_q\big(n,N-d(q-r)-k-dqj\big) - C_q\big(n,N-d(q-r)-k-dr-dqj\big)\big] \\ &\quad= \sum_{j=0}^{\infty}\big[C_q\big(n,d(q-r)+k+dqj\big) - C_q\big(n,d(q-r)+k+dr+dqj\big)\big]\end{aligned}$$

$$= \sum_{j=0}^{\infty} \big[C_q\big(n, k - dr + dq(j+1)\big) - C_q\big(n, k + dq(j+1)\big)\big]$$

$$= -\sum_{j=-\infty}^{-1} \big[C_q(n, k - dqj) - C_q(n, k - dr - dqj)\big]$$

$$= \gamma_q(n, d, r, k) - \Gamma_q(n, d, r, k) \qquad \square$$

Key to the calculations that follow is the following dimensional symmetry. Note that since $\dim B_N = 1$, the multiplication map induces a non-degenerate pairing $B_k \otimes B_{N-k} \to B_N \cong \mathbb{F}$. Let $\eta\colon B_N \to \mathbb{F}$ be an isomorphism.

**Lemma 4.2.** *The bilinear form* $\langle \cdot, \cdot \rangle\colon B_k\lambda^r \otimes B_{N-rd-k}\lambda^r \to \mathbb{F}$ *defined by* $\langle b\lambda^r, c\lambda^r \rangle = \eta(b\lambda^r c)$ *is non-degenerate. Hence* $\dim B_k\lambda^r = \dim B_{N-rd-k}\lambda^r$.

**Proof.** Let $\mu = \lambda^r$. Define first the form $\langle \cdot, \cdot \rangle_\mu\colon B_k \otimes B_{N-rd-k} \to \mathbb{F}$ by $\langle b, c \rangle_\mu = \eta(b\mu c)$. Then the left radical of this form is $\{b \in B_k \mid (b\mu)c = 0,\ \forall c \in B_{N-rd-k}\} = \{b \in B_k \mid b\mu = 0\} = \mathrm{Ann}(\mu) \cap B_k$. Similarly the right radical is $\mathrm{Ann}(\mu) \cap B_{N-rd-k}$. Since $B_k/(\mathrm{Ann}(\mu) \cap B_k) \cong B_k\mu$ and $B_{N-rd-k}/(\mathrm{Ann}(\mu) \cap B_{N-rd-k}) \cong B_{N-rd-k}\mu$, the result follows. $\square$

**Theorem 4.3.** *Suppose for some positive integer* $t$, *that* $H(\lambda^{q-1}, B_k) = 0$ *for all* $k \le t$. *Then* $H(\lambda^{q-r}, B_{k-d(r-1)}) = 0$ *for all* $1 \le r < q$ *and all* $k \le t$.

**Proof.** We use induction on $r$, the base case $r = 1$ being the hypothesis. Suppose $k \le t$ and take $a \in \mathrm{Ann}(\lambda^r) \cap B_{k-d(r-1)}$. Then $a\lambda^r = 0$, so $(a\lambda)\lambda^{r-1} = 0$. Thus $a\lambda \in \mathrm{Ann}(\lambda^{r-1}) \cap B_{k-d(r-2)}$. By the inductive hypothesis, $a\lambda = b\lambda^{q-r+1}$ for some $b \in B_{k-d(q-1)}$. Thus $(a - b\lambda^{q-r})\lambda = 0$ and $a - b\lambda^{q-r} \in B_{k-d(r-1)}$. From the hypothesis we deduce that there exists a $c$ such that $a - b\lambda^{q-r} = c\lambda^{q-1}$ which implies that $a \in \lambda^{q-r}B_{k-d(q-1)}$. Thus $\mathrm{Ann}(\lambda^r) \cap B_{k-d(r-1)} = \lambda^{q-r}B_{k-d(q-1)}$ and $H(\lambda^{q-r}, B_{k-d(r-1)}) = 0$. $\square$

**Corollary 4.4.** *Suppose that* $H(\lambda^{q-1}, B_k) = 0$ *for all* $k \le t$. *Then* $\dim B_k\lambda^r = \gamma_q(n, d, q-r, k)$ *for* $k \le t - d(r-1)$.

**Proof.** As observed above, it suffices to show that the complex

$$\cdots \xrightarrow{\lambda^{q-r}} B_{k-dq} \xrightarrow{\lambda^r} B_{k-d(q-r)} \xrightarrow{\lambda^{q-r}} B_k \xrightarrow{\lambda^r} B_k\lambda^r$$

is exact for $k \le t - d(r-1)$. The homology spaces of this complex are $H(\lambda^{q-r}, B_{k-dqj})$ and $H(\lambda^r, B_{k-d(q-r)-dqj})$ for $j \ge 0$. Since $k - dqj \le t - d(r-1)$ and $k - d(q-r) - dqj \le t - d(q-r-1)$ all of these spaces are zero by Theorem 4.3. $\square$

**Theorem 4.5.** *Suppose that* $H(\lambda^{q-1}, B_{k'}) = 0$ *for all* $k' \leq (N-d)/2$. *Then*

$$\dim H\big(\lambda^{q-1}, B_k\big) = \Gamma_q(n, d, q-1, k) \quad \text{for } k = \big\lfloor (N-d+2)/2 \big\rfloor$$

**Proof.** Set $k = \lfloor (N-d+2)/2 \rfloor$, so that $(N-d)/2 < k \leq (N-d+2)/2$. Note that

$$\begin{aligned} \dim H\big(\lambda^{q-1}, B_k\big) &= \dim\big(\mathrm{Ann}(\lambda) \cap B_k\big) - \dim \lambda^{q-1} B_{k-d(q-1)} \\ &= \dim B_k - \dim B_k\lambda - \dim B_{k-d(q-1)}\lambda^{q-1} \end{aligned}$$

Since $k > (N-d)/2$, we have $N-d-k < (N-d)/2$. Using Lemma 4.2 we see that

$$\dim B_k\lambda = \dim B_{N-d-k}\lambda = \gamma_q(n, d, q-1, N-d-k)$$

On the other hand, since $k \leq (N-d+2)/2$, we have $k-d(q-1) \leq (N-d+2)/2 - d(q-1) \leq (N-d)/2 - d(q-2)$. So $\dim B_{k-d(q-1)}\lambda^{q-1} = \gamma_q(n, d, 1, k-d(q-1))$. Putting all this together and using Lemma 4.1 yields

$$\begin{aligned} \dim H\big(\lambda^{q-1}, B_k\big) &= C_q(n,k) - \gamma_q(n, d, q-1, N-d-k) - \gamma_q\big(n, d, 1, k-d(q-1)\big) \\ &= \gamma_q(n, d, q-1, k) - \gamma_q(n, d, q-1, N-d-k) \\ &= \Gamma_q(n, d, q-1, k) \qquad \square \end{aligned}$$

In the quadratic case it is shown in [17] that if $q$ is prime and $\lambda$ has maximal rank, then the dimension of this space is always given by such a formula. In fact, in the maximal rank case

$$\dim H\big(\lambda^{q-r}, B_k\big) = \Gamma_q(n, 2, q-r, k) \quad \text{if } \frac{N}{2} - r < k < \frac{N}{2} + (q-r)$$

and is zero elsewhere. We expect something similar to hold in the higher degree case.

**Conjecture 1.** *If* $q$ *is prime, then for generic* $\lambda$,

$$\dim H\big(\lambda^{q-1}, B_k\big) = \begin{cases} 0 & \text{if } k \leq (N-d)/2 \\ \Gamma_q(n, d, q-1, k) & \text{if } (N-d)/2 < k < (N+(q-1)d)/2 \\ 0 & \text{if } k > (N+(q-1)d)/2 \end{cases}$$

We deliberately leave the definition of generic vague. Certainly we expect the conjecture to only hold if $\lambda$ has maximal rank in the following sense.

**Definition 4.6.** Let $\lambda$ be a homogeneous element of $B$. The *rank* of $\lambda$ is the smallest integer $s$ such that there exist $\mu_1, \ldots, \mu_s \in B_1$ with $\lambda \in \mathbb{F}[\mu_1, \ldots, \mu_s]$. That is, $s$ is the smallest number of linear elements required to generate $\lambda$.

In the quadratic case ($d = 2$), we know from [17] that the conjecture is true precisely when $\lambda$ has maximal rank. The proportion of quadratic polynomials in $n$ variables that have maximal rank is given by the $q$-Pochhammer symbol [5, Theorem 3.4]

$$\left(\frac{1}{q};\frac{1}{q^2}\right)_{\lfloor (n+1)/2\rfloor} = \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^3}\right)\cdots\left(1-\frac{1}{q^{1+2\lfloor (n-1)/2\rfloor}}\right)$$

which tends to 1 as $q$ tends to infinity. The proof used in [17] for the quadratic case relies heavily on the classification of quadratic forms. Since no such classification exists for higher degree forms, the proof cannot be generalized to the higher degree case ($d > 2$). When $d > 2$, experimental evidence suggests that the conjecture is true for most $\lambda$ but that being of maximal rank is no longer sufficient (see Appendix B). It also suggests that even when the conjecture fails, the differences between the actual and conjectured values of $\dim H(\lambda^{q-1}, B_k)$ are small.

In order to deduce information about the first fall degree we need information about the non-vanishing of $\Gamma_q(n, d, r, k)$.

**Theorem 4.7.** *If $2 \le d \le n(q-1)$, then*

$$\Gamma_q\big(n, d, q-1, (N-d+2)/2\big) > 0$$

**Proof.** See Appendix A. □

**Corollary 4.8.** *There exists an integer $k \le (N-d+2)/2$ such that $H(\lambda^{q-1}, B_k) \ne 0$.*

**Proof.** If $H(\lambda^{q-1}, B_{k'}) = 0$ for all $k' \le (N-d)/2$, then for $k = \lfloor (N-d+2)/2\rfloor$, $\dim H(\lambda^{q-1}, B_k) = \Gamma_q(n, d, q-1, k) > 0$ by Theorems 4.5 and 4.7. □

**Theorem 4.9.** *Let $\lambda$ be an element of degree $d$ and rank $s$. Then $D_{\mathrm{ff}}\lambda \le (s(q-1)+d+2)/2$.*

**Proof.** Without loss of generality we can assume that $\lambda \in \mathbb{F}[X_1, \ldots, X_s]$. Set $\tilde{B} = \mathbb{F}[X_1, \ldots, X_s]$ and $\hat{B} = \mathbb{F}[X_{s+1}, \ldots, X_n]$. Then

$$H\big(\lambda^{q-1}, B_k\big) \cong \bigoplus_i H\big(\lambda^{q-1}, \tilde{B}_{k-i}\big) \otimes \hat{B}_i$$

So $H(\lambda^{q-1}, \tilde{B}_k) \ne 0 \Rightarrow H(\lambda^{q-1}, B_k) \ne 0$. By Corollary 4.8, $H(\lambda^{q-1}, \tilde{B}_k) \ne 0$ for some $k \le (s(q-1) - d + 2)/2$. Hence the first fall degree of $\lambda$ in $B$ is less than or equal to $(s(q-1) - d + 2)/2 + d = (s(q-1) + d + 2)/2$. □

## 5. Weil descent

We now return to the setting of Weil descent. We have an operator $P\colon \mathbb{K}^m \to \mathbb{K}$ and a linear isomorphism that identifies $\mathbb{K}$ with $\mathbb{F}^n$. Through this isomorphism, an equation $P(X) = Y$ over $\mathbb{K}$ corresponds to a system of $n$ equations $p_1(x_{11}, \ldots, x_{mn}) = y_1$,

$\ldots, p_n(x_{11}, \ldots, x_{mn}) = y_n$. By Theorem 3.3, the first fall degree of this system is bounded by the first fall degree of the single polynomial $P_0$ as an element of $B = \mathbb{K}[X_{01}, \ldots, X_{n-1,m}]/\langle X_{01}^q, \ldots, X_{n-1,m}^q \rangle$. Recall that in Definition 4.6 we defined the rank of $P_0$ to be the smallest integer $r$ such that there exist $r$ linear elements $\ell_1, \ldots, \ell_r \in B_1$ for which $P_0 \in \mathbb{K}[\ell_1, \ldots, \ell_r]$. Combining Theorem 4.9 and Theorem 3.3 we obtain

**Theorem 5.1.** *Suppose* $\deg_{\mathbb{F}} P = d$ *and* $\operatorname{Rank} P_0 = s$. *Then*

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq \big(s(q-1) + d + 2\big)/2$$

For example if $P(X) = X_1^{1+q^{r_1}} + \cdots + X_m^{1+q^{r_m}}$, then $P$ is quadratic over $\mathbb{F}$, and $P_0 = X_{01}X_{r_1,1} + \cdots + X_{0m}X_{r_m,m}$ which has rank $2m$. Thus the first fall degree of the associated system is bounded by $m(q-1)+2$. In this case the bound is intuitive because we can see that $X_1^{q-1} \ldots X_m^{q-1} P(x)$ has degree $(m-1)(q-1)+2$ over $\mathbb{F}$, rather than the expected $m(q-1)+2$, so we have a degree fall.

Following [22] we look at the case where the degree of $P$ in any individual variable is bounded by $q^t - 1$. When $q = 2$, this theorem yields their result that $D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq mt + 1$.

**Theorem 5.2.** *Suppose that the degree of* $P$ *in any individual variable is bounded by* $q^t - 1$. *Then*

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq (q-1)mt + 1$$

*If further,* $\deg_{\mathbb{F}} P = d$, *then* $D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq (q-1)mt/2 + d/2 + 1$.

**Proof.** First note that the rank $s$ of $P_0$ is bounded by $mt$ since it is contained in the algebra generated by the $mt$ variables $X_{ji}$ for $i = 1, \ldots, m$ and $j = 0, \ldots, t-1$. So Theorem 5.1 implies that $D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq (q-1)mt/2 + d/2 + 1$. This proves the second assertion. To find the first bound it remains to bound $d$ when the degree of $P$ in any individual variable is bounded by $q^t - 1$.

The monomial in $X_i$ of maximal degree over $\mathbb{F}$ which has degree less than or equal to $q^t - 1$ is of course

$$X_i^{q^t-1} = \big(X_i . X_i^q \ldots X_i^{q^{t-1}}\big)^{q-1}$$

which has $\mathbb{F}$-degree $(q-1)t$. Thus the monomial of highest $\mathbb{F}$-degree that can occur in $P$ is

$$X_1^{q^t-1} \ldots X_m^{q^t-1}$$

and this has $\mathbb{F}$-degree $(q-1)mt$. Thus the degree $d = \deg_{\mathbb{F}} P$ is bounded by $(q-1)mt$. Hence,

$$D_{\mathrm{ff}}(p_1,\ldots,p_n) \leq \frac{mt(q-1)+(q-1)mt+2}{2} = (q-1)mt+1$$

as required. □

To see how the bound in Theorem 5.1 yields a much sharper bound in specific situations consider the quadratic operator over $\mathbb{F}_2$ given by

$$P(X_1,\ldots,X_m) = X_1X_1^{2^\theta} + \cdots + X_mX_m^{2^\theta}$$

The Petit–Quisquater bound (Theorem 5.2) in this situation is $(\theta+1)m+1$. However as we noticed above, Theorem 5.1 yields the much lower bound of $m+2$.

We now consider the single variable case and show that our result also generalizes the result for HFE systems given in [6].

**Lemma 5.3.** $\operatorname{Rank} P_0 \leq \lfloor \log_q(\deg P - d + 1)\rfloor + 1$.

**Proof.** Suppose that $P(X) = \sum_{k=0}^{D} a_k X^k$. Let $d = \deg_{\mathbb{F}} P$ and let $s = \operatorname{Rank} P_0$. Then $P$ must involve a monomial of degree at least $q^{s-1}$; otherwise $P_0$ would be contained in the sub-algebra generated by $X_0,\ldots,X_{s-2}$ and would have rank less than or equal to $s-1$. The lowest possible degree for a monomial of degree $d$ over $\mathbb{F}$ and involving $X^{q^{s-1}}$ is $q^{s-1}+(d-1)$. Hence $q^{s-1}+(d-1) \leq D$. Since $s-1$ is an integer, this implies that $s-1 \leq \lfloor \log_q(D-d+1)\rfloor$. In other words, $\operatorname{Rank} P_0 \leq \lfloor \log_q(\deg P - d + 1)\rfloor + 1$. □

**Theorem 5.4.** *Let* $P\colon \mathbb{K} \to \mathbb{K}$ *be a polynomial function with* $\deg_{\mathbb{K}} P = D$ *and* $\deg_{\mathbb{F}} P = d$. *Then*

$$D_{\mathrm{ff}}(p_1,\ldots,p_n) \leq \big((q-1)\lfloor \log_q(D-d+1)\rfloor + d + q + 1\big)/2$$

**Proof.** Lemma 5.3 and Theorem 5.1. □

In HFE cryptosystems, $P$ is quadratic over $\mathbb{F}$; so $d=2$. In this case the formula above reduces to the inequality

$$D_{\mathrm{ff}}(p_1,\ldots,p_n) \leq \big((q-1)\lfloor \log_q(D-1)\rfloor + q + 3\big)/2$$

which is the bound given in [6] for such systems.

Note that we do not expect the bound in Theorem 5.4 to be particularly sharp since the first fall degree of a vector space is generally less than the first fall degree of any particular member. For instance, consider the case when $q=2$ and $n=4$. Let $\lambda = x_1x_3 + x_2x_4$ and $\nu = x_1(x_2+x_3) + x_3x_4$. Let $V = \{0,\lambda,\nu,\lambda+\nu\}$ be the subspace generated by $\nu$ and $\lambda$. Then $\lambda, \nu$ and $\lambda+\nu$ all have a first fall degree of 4 because they have rank 4. However, $D_{\mathrm{ff}}(V) = 3$ since $x_2\lambda + x_3\nu = 0$.

## 6. Experimental results and perspectives

We now discuss the tightness of our bounds and the possible consequences of these bounds for the complexity of Gröbner basis algorithms on polynomial systems arising from a Weil descent. To this aim, we performed experiments using Magma's *GroebnerBasis* routine on various instances of the system of equations $p_1(x_{11}, \ldots, x_{mn}) = y_1, \ldots, p_n(x_{11}, \ldots, x_{mn}) = y_n$ augmented with the field equations $x_{ij}^q - x_{ij} = 0$.

### 6.1. Tightness of our bounds

We first study the tightness of the bounds computed in Section 5. In our experiments, we fixed $m = 1$ and we ran 100 experiments for various values of the parameters $n$, $d$ and $t$. For each experiment, we generated a random polynomial of degree $d$ over $\mathbb{F}$ and $D \leq q^t - 1$ over $\mathbb{K}$, and we solved the corresponding system using Magma's Gröbner basis routine. The value $B$ reported in Table 1 is the first fall degree bound $\lfloor((q-1)\lfloor \log_q(D - d+1)\rfloor + d + q + 1)/2\rfloor$ derived in this paper. The value $D_{\text{ff}}$ is the average first fall degree of the systems for the 100 experiments, as observed by looking at Magma's *verbose* output.

For each set of $p$, $t$, $d$ and $n$ values, we observed no variability at all in the first fall degree among the 100 experiments we performed. As expected, the actual first fall degree does not depend on $n$ in general, but seems to be completely determined by the parameters $p$, $t$ and $d$. The only exception we observed in our experiments occurs for the parameters $p = 3$, $t = 5$, $d = 2$, where the experimental first fall degree is smaller for $n = 11$ than for all larger $n$ values. The results of Table 1 also suggest that our upper bound on the first fall degree can be slightly improved. We leave as an open problem to either find a better upper bound or to exhibit some particular polynomials that would reach our bounds.

### 6.2. Gröbner basis algorithms

Gröbner basis algorithms essentially perform Gaussian elimination on Macaulay matrices. These matrices contain the coefficients of all polynomials $q_{i,j} := m_j p_i$ up to a certain degree, one row per polynomial, for all possible monomials $m_j$. The degree is progressively increased in the course of the algorithm, until new low degree polynomials and finally a Gröbner basis are found by linearization. At that time, the system can be easily solved when it has a small number of solutions.

Magma's Gröbner basis routine uses Faugère's F4 algorithm [11] by default. The algorithm proceeds in several steps to compute a degree reverse lexicographic ordering Gröbner basis, every step corresponding to a certain degree at which new polynomials are added. The algorithm first adds all polynomials up to the original maximal degree of the equations. It then performs linear algebra on the coefficients of these polynomials. If no polynomial of lower degree is obtained after the linear algebra step, then the degree

**Table 1**
Experimental first fall degrees and degrees of regularity. $B$ is the bound provided by Theorem 5.4; $D_{\text{ff}}$ and $D_{\text{reg}}$ are average values (over 100 experiments) of the experimental first fall degrees and degrees of regularity; $D_{\text{sr}}$ is the degree of regularity [1,24] of a semi-regular system of $n$ equations of degree $d$ in $n$ variables.

| $p$ | $t$ | $d$ | $n$ | $B$ | $D_{\text{ff}}$ | $D_{\text{reg}}$ | $D_{\text{sr}}$ |
|---|---|---|---|---|---|---|---|
| 2 | 6 | 2 | 11 | 5 | 4.0 | 4.0 | 4 |
| 2 | 6 | 2 | 13 | 5 | 4.0 | 4.0 | 4 |
| 2 | 6 | 2 | 17 | 5 | 4.0 | 4.0 | 5 |
| 2 | 6 | 3 | 11 | 5 | 5.0 | 5.0 | 5 |
| 2 | 6 | 3 | 13 | 5 | 5.0 | 5.0 | 6 |
| 2 | 6 | 3 | 17 | 5 | 5.0 | 5.0 | 7 |
| 2 | 6 | 4 | 11 | 6 | 5.0 | 5.0 | 6 |
| 2 | 6 | 4 | 13 | 6 | 5.0 | 5.0 | 7 |
| 2 | 6 | 4 | 17 | 6 | 5.0 | 5.1 | 8 |
| 2 | 6 | 5 | 11 | 6 | 6.0 | 6.0 | 7 |
| 2 | 6 | 5 | 13 | 6 | 6.0 | 6.0 | 8 |
| 2 | 6 | 5 | 17 | 6 | 6.0 | 6.0 | 9 |
| 2 | 7 | 2 | 11 | 5 | 4.0 | 4.0 | 4 |
| 2 | 7 | 2 | 13 | 5 | 4.0 | 4.0 | 4 |
| 2 | 7 | 2 | 17 | 5 | 4.0 | 4.0 | 5 |
| 2 | 7 | 3 | 11 | 6 | 5.0 | 5.0 | 5 |
| 2 | 7 | 3 | 13 | 6 | 5.0 | 5.0 | 6 |
| 2 | 7 | 3 | 17 | 6 | 5.0 | 5.0 | 7 |
| 2 | 7 | 4 | 11 | 6 | 6.0 | 6.0 | 6 |
| 2 | 7 | 4 | 13 | 6 | 6.0 | 6.0 | 7 |
| 2 | 7 | 4 | 17 | 6 | 6.0 | 6.0 | 8 |
| 2 | 7 | 5 | 11 | 7 | 6.0 | 6.0 | 7 |
| 2 | 7 | 5 | 13 | 7 | 6.0 | 6.0 | 8 |
| 2 | 7 | 5 | 17 | 7 | 6.0 | 6.1 | 9 |
| 2 | 7 | 6 | 11 | 7 | 7.0 | 7.0 | 8 |
| 2 | 7 | 6 | 13 | 7 | 7.0 | 7.0 | 9 |
| 2 | 7 | 6 | 17 | 7 | 7.0 | 7.0 | 10 |

| $p$ | $t$ | $d$ | $n$ | $B$ | $D_{\text{ff}}$ | $D_{\text{reg}}$ | $D_{\text{sr}}$ |
|---|---|---|---|---|---|---|---|
| 3 | 3 | 2 | 11 | 5 | 4.0 | 4.7 | 5 |
| 3 | 3 | 2 | 13 | 5 | 4.0 | 4.5 | 6 |
| 3 | 3 | 2 | 17 | 5 | 4.0 | 4.5 | 7 |
| 3 | 3 | 2 | 19 | 5 | 4.0 | 4.5 | 7 |
| 3 | 3 | 2 | 23 | 5 | 4.0 | 4.8 | 8 |
| 3 | 3 | 2 | 29 | 5 | 4.0 | 4.7 | 9 |
| 3 | 4 | 2 | 11 | 6 | 5.0 | 5.2 | 5 |
| 3 | 4 | 2 | 13 | 6 | 5.0 | 5.7 | 6 |
| 3 | 4 | 2 | 17 | 6 | 5.0 | 5.9 | 7 |
| 3 | 4 | 2 | 19 | 6 | 5.0 | 6.0 | 7 |
| 3 | 4 | 2 | 23 | 6 | 5.0 | 6.0 | 8 |
| 3 | 4 | 3 | 11 | 7 | 6.0 | 6.6 | 7 |
| 3 | 4 | 3 | 13 | 7 | 6.0 | 6.6 | 8 |
| 3 | 4 | 3 | 17 | 7 | 6.0 | 6.4 | 10 |
| 3 | 4 | 3 | 19 | 7 | 6.0 | 6.8 | 10 |
| 3 | 4 | 3 | 23 | 7 | 6.0 | 6.8 | 12 |
| 3 | 5 | 2 | 11 | 7 | 5.0 | 5.2 | 5 |
| 3 | 5 | 2 | 13 | 7 | 6.0 | 6.4 | 6 |
| 3 | 5 | 2 | 17 | 7 | 6.0 | 6.6 | 7 |
| 3 | 5 | 2 | 19 | 7 | 6.0 | 6.8 | 7 |
| 3 | 5 | 3 | 11 | 8 | 7.0 | 7.6 | 7 |
| 3 | 5 | 3 | 13 | 8 | 7.0 | 7.4 | 8 |
| 3 | 5 | 3 | 17 | 8 | 7.0 | 7.7 | 10 |
| 3 | 5 | 4 | 11 | 8 | 7.0 | 7.6 | 9 |
| 3 | 5 | 4 | 13 | 8 | 7.0 | 7.7 | 10 |

is increased by one in the next step, otherwise the degree may either stay unchanged or even be decreased in the next step. Eventually when a degree reverse lexicographic ordering Gröbner basis has been found, Magma's Gröbner basis routine uses FGLM algorithm [13] to convert it into a lexicographic Gröbner basis.

When the system has few solutions, the cost of FGLM can be neglected and the complexity of Gröbner basis algorithms can be estimated by the cost of linear algebra. This cost is bounded by $(mn)^{\omega D_{\text{reg}}}$ in our case, where $mn$ is the number of variables, $\omega$ is the linear algebra constant and $D_{\text{reg}}$ is the maximal degree occurring in the algorithm before it successfully terminates. This degree called the *degree of regularity* of the system, is therefore a very important complexity parameter. Finding rigorous bounds for the degree of regularity has proved to be a difficult problem, though effective bounds have been found in a number of special cases [1,4,8,10].

The *first fall degree* studied in this paper corresponds to the first degree at which the F4 algorithm will find non-zero "low degree" polynomials, and where it will therefore

(at least temporarily) not increase the degree in the next step. The first fall degree provides a lower bound on the degree of regularity and is often easier to evaluate. At first sight, this degree provides only a lower bound on the complexity of Gröbner basis algorithms. However when not only one but *many* non-trivial degree falls occur at the first fall degree, Gröbner basis algorithms may quickly terminate after this degree is reached, and the first fall degree may therefore be a reasonable approximation of the degree of regularity.

### *6.3. First fall degree and degree of regularity*

We then investigate the heuristic assumption that the first fall degree is a good approximation of the degree of regularity for polynomial systems arising from a Weil descent. This assumption was explicitly taken in [22] and more or less explicitly taken in several previous works on HFE [7,6,16]. The conjecture that binary ECDLP is subexponential in [22] or that inverting HFE is quasi-polynomial in [7,6,16] crucially require at least a relaxed version of this assumption (on a family of polynomials with increasing degrees and number of variables in the ECDLP case), so it is very important to establish to what extent it might be true. (An alternative approach to establishing quasi-polynomial complexity for HFE systems is described in [2] where it is shown that quasi-polynomiality follows from a version of Fröberg's conjecture.)

In Table 1, we report the maximal degree $D_{\mathrm{reg}}$ reached by the Gröbner basis routine, averaged over our 100 experiments. For comparison, we provide the value $D_{\mathrm{sr}}$ of the degree of regularity of a semi-regular system of equations of degree $d$ in $n$ variables over $\mathbb{F}_p$ [1,24]

$$D_{\mathrm{sr}} = \min\left\{d \;\middle|\; \left[t^d\right]\left(\left(1-t^p\right)^n\left(1-t^2\right)^m\right)/\left(\left(1-t\right)^n\left(1-t^{2p}\right)^m\right) \leq 0\right\}$$

(that is, $D_{\mathrm{sr}}$ is the degree of the first power of $t$ in the expansion of $(1-t^p)^n(1-t^2)^m/((1-t)^n(1-t^{2p})^m)$ whose coefficient is non-positive). We observe that as $d$ and $n$ grow the average experimental degree of regularity diverges from the degree of regularity of semi-regular systems whereas it remains close to the observed first fall degree. This provides some evidence in favor of the assumption that the first fall degree is a good approximation of the degree of regularity for polynomial systems arising from a Weil descent.

We note that under this assumption, the results of Section 5 provide a heuristic upper bound $(nm)^{\omega O(D_{\mathrm{ff}})}$ on the complexity of Gröbner basis algorithms on the systems considered in this paper, where $2 \leq \omega < 3$ is the linear algebra constant. A better upper bound $n^{\omega O(D_{\mathrm{ff}})}$ can be obtained using the block structure of the systems [14,22]. In particular if $q$ and $d$ are fixed and if $D$ is polynomial in $n$, then by Theorem 5.4, the complexity of solving such systems is then bounded by $2^{O(\log^2(n))}$ which is quasi-polynomial in $n$.

## 7. Conclusion

We have given a universal bound on the first fall degree of a system of equations arising from Weil descent.

$$D_{\mathrm{ff}}(P) \leq \big((q-1)\log_q(D-d+1)+d+q+1\big)/2$$

where $q$ is the order of the base field, $D$ is the degree of the univariate polynomial $P$ and $d$ is its degree over the base field. This formula generalizes that given in [6] when $d=2$.

We have then conducted experiments on several systems of this kind. The experimental results suggest that our bound could be slightly improved in further work. Moreover, they suggest that a heuristic assumption appearing in previous works [22,7,6,16] could be satisfied in our setting as well, at least for all the parameters we could test. Under this assumption, the complexity of the direct algebraic attack can be estimated by $n^{O(3D_{\mathrm{ff}})}$. In the standard view of HFE systems, $q$ and $d$ are fixed and $D$ is polynomial in $n$. Our result then implies that the complexity in this situation is quasi-polynomial in $n$.

The heuristic assumption needed to obtain this complexity is that Gröbner basis algorithms terminate at a degree only slightly higher than the first fall degree defined here. Our theoretical understanding of the first fall degree has grown substantially over the last few years, yet little progress has been made on quantifying precisely the connection between the first fall degree and the termination of these algorithms. It would be extremely useful to have some kind of probabilistic bound on the difference between these two degrees.

## Appendix A. Proof of non-vanishing of $\Gamma_q(n,d,r,k)$

We now give a brief proof of Theorem 4.7. Define $PC_q(n,r,k)=\sum_{j=-\infty}^{\infty} C_q(n,k+rj)$ so that

$$\Gamma_q(n,d,r,k) = PC_q(n,dq,k) - PC_q(n,dq,k-dr)$$

**Lemma A.1.** *Let $q,d,n$ and $r$ be positive integers then $\Gamma_q(n,d,r,k)$ is anti-symmetric about $(N+dr)/2$. That is,*

$$\Gamma_q(n,d,r,N+dr-k) = -\Gamma_q(n,d,r,k)$$

**Proof.** Since $C_q(n,N-k)=C_q(n,k)$, we also have $PC_q(n,N-k)=PC_q(n,k)$. Then

$$\begin{aligned}\Gamma_q(n,d,r,N+dr-k) &= PC_q(n,dq,N+dr-k) - PC_q(n,dq,N+dr-k-dr)\\ &= PC_q(n,dq,k-dr) - PC_q(n,dq,k)\\ &= -\Gamma_q(n,d,r,k) \qquad \square\end{aligned}$$

We split the proof of Theorem 4.7 into two cases, when $d > n$ and when $d \leq n$. The reason for this is that when $d > n$, the period $dq$ exceeds $n(q-1)$ and so $PC_q(n, dq, k)$ trivializes to $C_q(n, k)$ and is zero some of the time. When $n > d$ the behavior of $\Gamma_q(n, d, r, k)$ is much more complicated and we need for our inductive hypothesis that $\Gamma_q(n, d, r, )$ be strictly increasing. This is not true when $d > n$ due to the trivialization.

**Proposition A.2.** *Let $q, n$ and $d$ be positive integers such that $n < d \leq n(q-1)$. Then*

$$\Gamma_q\left(n, d, q-1, \frac{N-d+2}{2}\right) > 0$$

**Proof.** Note that since $d > n$, we have that $dq > n(q-1)+1$. For an integer $b$ let $b'$ be the least positive residue modulo $dq$. Hence $PC_q(n, dq, k) = C_q(n, k')$. Let $k = (N-d+2)/2$ and note $0 < k < dq$ but also

$$\Gamma_q(n, d, q-1, k) = C_q(n, k) - C_q\big(n, \big(k - d(q-1)\big)'\big)$$

if $k - d(q-1) > 0$ we are done because $C_q$ is increasing on $[0, N/2]$. If $k - d(q-1) < 0$ then $k + d$ is the least positive residue. So we need to demonstrate that

$$C_q(n, k) > C_q(n, k+d)$$

which by the symmetry of $C_q$ about $N/2$ amounts to showing

$$|k - N/2| < |k + d - N/2|$$

We see

$$|k - N/2| = \left|\frac{N-d+2-N}{2}\right| = \left|\frac{2-d}{2}\right| < \left|\frac{d+2}{2}\right| = |k + d - N/2| \qquad \square$$

**Theorem A.3.** *Let $q, n, r$ and $d$ be positive integers such that $1 < d \leq n$. Then for $k$ in the range*

$$\left(\frac{N - d(q-r)}{2}, \frac{N + dr}{2}\right)$$

*we have that $\Gamma_q(n, d, r, k) > 0$.*

**Proof.** Fix $q, r$ and $d$ as positive integers such that $q, d > 1$ and $0 < r < q$. We proceed by induction on $n$ beginning with the base case $n = d$. First note that since $d = n$ our interval is

$$\left(\frac{d(q-1) - d(q-r)}{2}, \frac{d(q-1) + dr}{2}\right) = \left(\frac{d(r-1)}{2}, \frac{d(q+r-1)}{2}\right)$$

Note that $C_q(d,k)$ is only non-zero for $k$ in the range $[0, d(q-1)]$ and that if $k \in [0, dq)$ then $PC_q(d, qd, k) = C_q(d,k)$.

Let $k \in (d(r-1)/2, d(q+r-1)/2)$. Suppose first that $k \leq N/2$ and write $k = N/2 - j$ where $0 \leq j \leq N/2$. Then

$$\Gamma_q(n,d,r,k) = \begin{cases} C_q(d,k) - C_q(d,k-dr) & \text{if } dr \leq k \\ C_q(d,k) - C_q(d,k-dr+dq) & \text{if } dr > k \end{cases}$$

Note that (as a function of $k$) $C_q(d,k)$ is symmetric about $d(q-1)/2$ and increasing on $[0, d(q-1)/2]$. So to show that $\Gamma_q(d,d,r,k) > 0$ it suffices to show that $k - dr + dq$ cannot lie in the range $[N/2 - j, N/2 + j]$ if $dr > k$. But

$$k > d(r-1)/2 \quad \Rightarrow \quad N/2 - j = d(q-1)/2 - j > d(r-1)/2 \quad \Rightarrow \quad d(q-r) > 2j$$

Hence $k - dr + dq = N/2 - j + d(q-r) > N/2 + j$. A similar argument works when $k > N/2$. This proves the result in the case $n = d$.

Now take $n > d$ and set $N' = (n-1)(q-1)$. The inductive hypothesis states that $\Gamma_q(n-1,d,r,k) > 0$ if $k \in ((N' - d(q-r))/2, (N' + dr)/2)$. Let $k \in ((N - d(q-r))/2, (N + dr)/2)$. Note that $\Gamma_q$ satisfies the $q$-nomial recurrence relation

$$\Gamma_q(n,d,r,k) = \sum_{i=0}^{q-1} \Gamma_q(n-1,d,r,k-i)$$

In order for terms on the right hand side to be negative we must have either $k \geq (N' + dr)/2$ or $k - q + 1 \leq (N' - d(q-r))/2$. Suppose that $k \geq (N' + dr)/2$ and let $s = k - (N' + dr)/2$. Then $2s < q - 1$ and the antisymmetry of Lemma A.1 implies that $\sum_{i=0}^{2s} \Gamma_q(n-1,d,r,k-i) = 0$. Since the remaining terms of the summation must be positive by the inductive hypothesis, we can conclude that $\Gamma_q(n,d,r,k) > 0$. A similar argument works in the case when $k - q + 1 \leq (N' - d(q-r))/2$. □

## Appendix B. Examples of $\dim H(\lambda^{q-r}, B_k)$

Conjecture 1 proposed a formula for values of $\dim H(\lambda^{q-r}, B_k)$ when $q$ is prime and $\lambda$ is generic in some sense. An analysis of 30 randomly chosen polynomials in the case $q = 7$, $n = 5$, $m = 1$ and $d = 6$ found that the conjecture held in 22 of these cases. For the eight polynomials for which the conjecture failed, the values of $\dim H(\lambda^{q-r}, B_k)$ differed from the conjectured values in 2–6 different positions. Two examples are given in Table 2 with the values which differed from the conjectured values given in red (in the web version). The conjectured values in each case were 0.

Similar results were found for smaller values of $q$, $n$ and $d$.

**Table 2**
dim $H(\lambda^{q-r}, B_k)$.

| | $q-r$ | | | | | | $q-r$ | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 0 | 0 | 0 | 0 | 5 | 5 | 0 | 0 | 0 | 0 | 5 | 5 |
| 2 | 0 | 0 | 0 | 0 | 15 | 15 | 0 | 0 | 0 | 0 | 15 | 15 |
| 3 | 0 | 0 | 0 | 0 | 35 | 35 | 0 | 0 | 0 | 1 | 35 | 35 |
| 4 | 0 | 0 | 0 | 55 | 70 | 70 | 0 | 0 | 0 | 55 | 70 | 70 |
| 5 | 0 | 0 | 0 | 121 | 126 | 126 | 0 | 0 | 0 | 121 | 126 | 126 |
| 6 | 0 | 0 | 0 | 209 | 210 | 209 | 0 | 0 | 1 | 209 | 210 | 209 |
| 7 | 0 | 0 | 199 | 325 | 325 | 320 | 0 | 0 | 199 | 325 | 325 | 320 |
| 8 | 0 | 0 | 400 | 470 | 470 | 455 | 0 | 0 | 400 | 470 | 470 | 455 |
| 9 | 0 | 0 | 605 | 640 | 640 | 605 | 0 | 0 | 605 | 640 | 640 | 605 |
| 10 | 0 | 356 | 811 | 826 | 826 | 756 | 0 | 356 | 811 | 826 | 826 | 756 |
| 11 | 0 | 690 | 1010 | 1015 | 1015 | 889 | 0 | 690 | 1010 | 1015 | 1015 | 889 |
| 12 | 1 | 980 | 1189 | 1190 | 1189 | 980 | 0 | 980 | 1189 | 1190 | 1189 | 980 |
| 13 | 315 | 1204 | 1330 | 1330 | 1325 | 1005 | 315 | 1204 | 1330 | 1330 | 1325 | 1005 |
| 14 | 594 | 1350 | 1420 | 1420 | 1405 | 950 | 594 | 1350 | 1420 | 1420 | 1405 | 950 |
| 15 | 811 | 1416 | 1451 | 1451 | 1416 | 811 | 811 | 1416 | 1451 | 1451 | 1416 | 811 |
| 16 | 950 | 1405 | 1420 | 1420 | 1350 | 594 | 950 | 1405 | 1420 | 1420 | 1350 | 594 |
| 17 | 1005 | 1325 | 1330 | 1330 | 1204 | 315 | 1005 | 1325 | 1330 | 1330 | 1204 | 315 |
| 18 | 980 | 1189 | 1190 | 1189 | 980 | 1 | 980 | 1189 | 1190 | 1189 | 980 | 0 |
| 19 | 889 | 1015 | 1015 | 1010 | 690 | 0 | 889 | 1015 | 1015 | 1010 | 690 | 0 |
| 20 | 756 | 826 | 826 | 811 | 356 | 0 | 756 | 826 | 826 | 811 | 356 | 0 |
| 21 | 605 | 640 | 640 | 605 | 0 | 0 | 605 | 640 | 640 | 605 | 0 | 0 |
| 22 | 455 | 470 | 470 | 400 | 0 | 0 | 455 | 470 | 470 | 400 | 0 | 0 |
| 23 | 320 | 325 | 325 | 199 | 0 | 0 | 320 | 325 | 325 | 199 | 0 | 0 |
| 24 | 209 | 210 | 209 | 0 | 0 | 0 | 209 | 210 | 209 | 1 | 0 | 0 |
| 25 | 126 | 126 | 121 | 0 | 0 | 0 | 126 | 126 | 121 | 0 | 0 | 0 |
| 26 | 70 | 70 | 55 | 0 | 0 | 0 | 70 | 70 | 55 | 0 | 0 | 0 |
| 27 | 35 | 35 | 0 | 0 | 0 | 0 | 35 | 35 | 1 | 0 | 0 | 0 |
| 28 | 15 | 15 | 0 | 0 | 0 | 0 | 15 | 15 | 0 | 0 | 0 | 0 |
| 29 | 5 | 5 | 0 | 0 | 0 | 0 | 5 | 5 | 0 | 0 | 0 | 0 |
| 30 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

## References


[1] M. Bardet, J.-C. Faugère, B. Salvy, B.-Y. Yang, Asymptotic behaviour of the degree of regularity of semi-regular systems of equations, in: Mega 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005, pp. 1–14.

[2] L. Bettale, J.-C. Faugère, L. Perret, Cryptanalysis of multivariate and odd-characteristic HFE variants, in: D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi (Eds.), Public Key Cryptography, PKC 2011, in: Lect. Notes Comput. Sci., vol. 6571, Springer, Berlin, 2011, pp. 441–458.

[3] L. Bettale, J.-C. Faugère, L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, Des. Codes Cryptogr. 69 (2012) 1–52.

[4] J. Buchmann, A. Pyshkin, R.-P. Weinmann, A zero-dimensional Gröbner basis for AES-128, in: FSE 2006, in: Lect. Notes Comput. Sci., vol. 4047, 2006, pp. 78–88.

[5] L. Carlitz, Representations by quadratic forms in a finite field, Duke Math. J. 21 (1954) 123–137.

[6] J. Ding, T.J. Hodges, Inverting the HFE systems is quasipolynomial for all fields, in: Advances in Cryptology, Crypto 2011, in: Lect. Notes Comput. Sci., vol. 6841, Springer, Berlin, 2011, pp. 724–742.

[7] V. Dubois, N. Gama, The first fall degree of HFE systems, in: M. Abe (Ed.), Advances in Cryptology, 16th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2010, in: Lect. Notes Comput. Sci., vol. 6477, Springer, Berlin, 2010, pp. 557–576.

[8] J.-C. Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer, Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology, in: ISSAC 2010, 2010, pp. 257–264.

[9] J.-C. Faugère, A. Joux, Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases, in: D. Boneh (Ed.), Advances in Cryptology, CRYPTO 2003, in: Lect. Notes Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 44–60.

[10] J.-C. Faugère, A. Joux, L. Perret, J. Treger, Cryptanalysis of the hidden matrix cryptosystem, in: LATINCRYPT 2010, 2010, pp. 241–254.
[11] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), J. Pure Appl. Algebra 139 (1999) 61–89.
[12] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: Proc. ISSAC 2002, New York, NY, USA, 2002, pp. 75–83.
[13] J.-C. Faugère, Patrizia M. Gianni, Daniel Lazard, Teo Mora, Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. Symb. Comput. 16 (1993) 329–344.
[14] J.-C. Faugère, Ludovic Perret, Christophe Petit, Guenael Renault, New subexponential algorithms for factoring in $SL(2, \mathbb{F}_{2^n})$, http://eprint.iacr.org/2011/598, 2011.
[15] J.-C. Faugère, Ludovic Perret, Christophe Petit, Guenael Renault, Improving the complexity of index calculus algorithms in elliptic curves over binary fields, in: EUROCRYPT 2012, in: Lect. Notes Comput. Sci., vol. 7237, 2012, pp. 27–44.
[16] L. Granboulan, A. Joux, J. Stern, Inverting HFE is quasi-polynomial, in: C. Dwork (Ed.), Advances in Cryptology, CRYPTO 2006, in: Lect. Notes Comput. Sci., vol. 4117, Springer, Berlin, 2006, pp. 345–356.
[17] T.J. Hodges, J. Schlather, The degree of regularity of a quadratic polynomial, J. Pure Appl. Algebra 217 (2013) 207–217.
[18] R. Lidl, H. Niederreiter, Finite Fields, Encycl. Math. Appl., vol. 20, Cambridge University Press, 1997.
[19] J. Patarin, Hidden field equations and isomorphism of polynomials (IP): two new families of asymmetric algorithms, in: U. Maurer (Ed.), Eurocrypt '96, in: Lect. Notes Comput. Sci., vol. 1070, Springer, Berlin, 1996, pp. 33–48.
[20] J. Patarin, L. Goubin, Asymmetric cryptography with Sboxes, in: Proc. ICICS'97, Beijing, China, in: Lect. Notes Comput. Sci., vol. 1334, 1997, pp. 369–380.
[21] J. Patarin, L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in: Proc. ICICS'97, Beijing, China, in: Lect. Notes Comput. Sci., vol. 1334, 1997, pp. 356–368.
[22] Christophe Petit, Jean-Jacques Quisquater, On polynomial systems arising from a Weil descent, in: X. Wang, K. Sako (Eds.), ASIACRYPT 2012, in: Lect. Notes Comput. Sci., vol. 7658, 2012, pp. 451–466.
[23] J. Riordan, An Introduction to Combinatorial Analysis, Dover, 2002.
[24] J.Y.-C. Yeh, C.-M. Cheng, B.-Y. Yang, Operating degrees for XL vs. $\mathbf{F_4}/\mathbf{F_5}$ for generic $\mathcal{MQ}$ with number of equations linear in that of variables, in: Number Theory and Cryptography Workshop, TU Darmstadt, Germany, November 21–22, 2013, in: Lect. Notes Comput. Sci., vol. 8260, 2013, pp. 19–33.
[25] X. Zhao, D. Feng, Bypassing the decomposition attacks on two-round multivariate schemes by a practical cubic round, IET Inf. Secur. 4 (3) (September 2010) 167–184.